ACCESS
or Excess?

BUSINESSES STRUGGLE TO ADDRESS THE POTENTIAL ABUSES OF SOCIAL MEDIA

The benefits of social media have been spelled out in great detail, especially their ability to build relationships, strengthen an organization's brand, promote events or products and to stay in constant contact (no pun intended) with customers. Yet detractors call them a time waster, a productivity killer and a serious threat to organizational security.

By Kate McDermott

"Constant Interruptions from social media impact employees' ability to engage in deep and creative thinking."

So What's a Business to Do?

Even the harshest critics of social media admit there is no turning back the clock. Social media are here to stay. Facebook and Twitter may be the current titans of the social networking world, but new platforms are being launched at a blistering pace. Yet, as is so often the case with advances in technology, many organizations have found that the benefits also come with some liabilities.

A March 2011 survey by the market research firm uSamp of 515 email users in U.S. companies of all sizes revealed that:

- Using, switching between and coordinating social media tools such as email, social networks, text messaging and instant messaging accounts for the majority of workplace distractions.

- In fact, 45 percent of respondents said they generally keep at least six items open at the same time on their desktop. Another 65 percent admitted they use one to three desktop or mobile devices in addition to their main computer.

- More than half of those polled (53 percent) reported they waste at least one hour a day due to these workplace distractions.

- A 2009 survey by Nucleus Research showed that organizations allowing employees to access Facebook at work lost an average of 1.5 percent in total employee productivity, with 87 percent of those surveyed revealing they often had no clear business reason for using the social network.

- The same Nucleus survey revealed that one in every 33 workers polled built their entire Facebook profile during work hours.

The IMpact to the Bottom Line

The sales and marketing benefits of social media have been well documented, but what about their negative impacts on an organization's bottom line? The uSamp survey calculated that the one hour a day the survey respondents wasted due to workplace distractions cost their businesses $10,375 per employee per year (based on an average hourly salary of $30/hour). For companies with just 100 employees, that results in more than $1 million in lost productivity each year.

Constant interruptions from tweets, Facebook postings and other social media alerts impact employees' ability to engage in deep and creative thinking and often result in information overload. Is it any surprise that productivity suffers?

In addition to productivity losses, many critics say social media foster a false sense of security that may leave organizations vulnerable to hacking, leaks of sensitive information or computer viruses. Employees posting information on Facebook instead of using email may knowingly or unwittingly circumvent corporate communication policies and privacy regulations.

A 2010 report by the IT security firm Sophos revealed an increase in attacks by social networking users, with 36 percent of those surveyed reporting they had received malware via social networking sites, an increase of 69.8 percent over the year before. Given numbers like that, it should come as no shock that nearly three quarters of the firms polled expressed concern that social networking sites leave their businesses—and their data—in jeopardy.

Even LinkedIn, considered by many to be the social media platform least threatened by hackers, can lead cyber crooks to a virtual corporate directory of staff names and positions—and their computers.

And of course, there is always the danger of posting personal information on a site that is also seen by business associates. Should employees be exposed (sometimes literally) to what their coworkers wore—or did not wear—on their summer vacations?

The Unsocial Side of Social Media

For those old enough to remember life pre-smartphones, laptops and iPads, boring meetings were endured by endless doodling (while pretending to take notes) or for the boldest (or most foolish), not very well-disguised nodding off.

Today, who needs pens and naps when employees can surf the web, answer emails or tweet during a meeting? In fact, two out of three uSamp survey respondents admitted to answering email or a mobile phone, chatting on IM, tweeting or updating their status on Facebook during a group meeting. Most, but not all, disconnect only when asked by a boss or during one-on-one meetings.

Mary Ellen Hackett, an account director for a D.C.-based public relations agency, says the challenge for employees today is balance. "Because media enables us to be so connected, I think there is an expectation that we should be able to remain on top of projects B, C and D even while we're working on project A. You have to multitask," she says. But there are times when Hackett is committed to disconnecting. "When I'm engaged in client interaction, it's a no-interruption zone."

The debate around proper social media etiquette is certainly not new, with critics charging that social media and the constant need to be "plugged in" has resulted in impatience and rampant inconsideration for others.

Mental health professionals say the problem goes even deeper. Psychologists have identified what they call "online compulsive disorder." The inability to disconnect from technology and connect with other humans is especially pervasive among those under 40, with the uSamp survey revealing that the majority of Millennials and beyond stay connected in bed and 44 percent of those under 30 admitting that they do not even log off during a night at the movies.

The Answer?

As the potential for abusing social media in the workplace has become more obvious, the pendulum has swung widely in terms of the best ways to handle

What's Your Policy?

Intel, the leading manufacturer of computer chips and processors, has made its social media guidelines accessible to the public and many companies use them as the model for their own practices.

Here is an abbreviated version of Intel's "rules of engagement:" 👍 Like

Be transparent. Your honesty—or dishonesty—will be quickly noticed in the social media environment. Use your real name, identify that you work for Intel, and be clear about your role.

Be judicious. Make sure your efforts to be transparent don't violate Intel's privacy, confidentiality, and legal guidelines for external commercial speech. All statements must be true and not misleading and all claims must be substantiated and approved. What you publish is widely accessible and will be around for a long time, so consider the content carefully.

Write what you know. Make sure you write and post about your areas of expertise.

Perception is reality. In online social networks, the lines between public and private, personal and professional are blurred. Just by identifying yourself as an Intel employee, you are creating perceptions about your expertise. Do us all proud.

It's a conversation. Talk to your readers like you would talk to real people in professional situations. Encourage comments. You can also broaden the conversation by citing others who are blogging about the same topic and allowing your content to be shared or syndicated.

Are you adding value? Social communication from Intel should help our customers, partners, and co-workers. It should be thought-provoking and build a sense of community.

Be a leader. There can be a fine line between healthy debate and incendiary reaction. Do not denigrate our competitors or Intel. Nor do you need to respond to every criticism or barb. Once the words are out there, you can't really get them back. And once an inflammatory discussion gets going, it's hard to stop.

Your responsibility: What you write is ultimately your responsibility. Participation in social computing on behalf of Intel is not a right but an opportunity, so please treat it seriously and with respect.

Did you screw up? If you make a mistake, admit it. Be upfront and be quick with your correction.

If it gives you pause, pause. If you're about to publish something that makes you even the slightest bit uncomfortable, don't shrug it off and hit 'send.' Take a minute to review these guidelines and try to figure out what's bothering you, then fix it. Ultimately, what you publish is yours—as is the responsibility. So be sure.

Close to half of the organizations polled allow their staff uncontrolled access to Facebook.

the problem. Just last year, the U.S. military issued a new policy that reversed its ban on some of the most popular social media websites. It seems even Uncle Sam recognizes the recruiting power of Facebook and YouTube (not to mention their morale-boosting powers).

And he was not alone. The 2010 security threat report by Sophos revealed that close to half of the respondent organizations allow their staff uncontrolled access to Facebook, an increase of 13 percent from the year earlier.

"A couple of years ago, before social media was a well-defined term, we had a policy that blocked sites we believed weren't appropriate for the workplace," says Andy Smith, director of marketing and communications for 270net Technologies, a Frederick-based web development firm. "But then, as these sites became tools for business, we began to recognize a legitimate use for them and unblocked certain sites. Now we encourage all our employees to use social media within certain guidelines that we modeled off of Intel's social media guidelines" (see sidebar).

But companies continue to struggle in their efforts to find a happy medium between access

and excess. Many are looking for ways to minimize the impact on productivity caused by digital distractions, with the primary strategy being blocking access to networks such as Facebook and/or other non-business websites.

Some are pursuing other "social security" measures, including programs that track online usage patterns as well as company-wide efforts to disconnect, such as No Facebook Fridays. There are also software applications that enable businesses to give their employees predetermined (and timed) access to social networking sites.

Managing New Media the Old-Fashioned Way

For many organizations, however, it still comes down to the boss' watchful eye. Don Francis, interim vice president for administration at Frederick Community College, says the institution does not have a formal policy regarding the use of social media. "We have an IT policy called an 'acceptable use' that recognizes that there are certain circumstances when personal use of computers is appropriate," he says. "We have a relatively small staff and we are extremely busy, so it's fairly easy to

gauge when someone is working efficiently and producing and when they are not. If and when it becomes a problem, it is addressed at the supervisory level."

The same is true at Montgomery College. Marcus S. Rosano, the school's media relations specialist, says the institution currently does not have formal policies regarding the use of social media. "Supervisors and managers are responsible for their employees' performance and productivity," he says, noting that employees are expected to follow policies related to the proper use of all college resources—including computers.

Smith says 270net Technologies developed its social media policy to take a proactive approach to dealing with employees who may abuse technology and thus hurt the company's bottom line. "Although I personally haven't had to take an individual aside (to address social media abuses), I won't say it hasn't happened," says Smith. "That's why we created our policy. We don't want people wasting time and there is always that risk." ∎

Kate McDermott is a freelance writer in Frederick, Md., and assistant editor of Frederick Magazine.